


AMENDMENTS TO THE CLAIMS

1. (Currently Amended) An apparatus for selectively encrypting data for transmission over a network in packets between a server and a client, the apparatus comprising:
a parser configured to parse a payload portion of the data in a packet from a non-payload portion of the packet data;
an encrypter configured to determine if the payload portion of the packet data is to be encrypted by examining the payload portion of the packet data to recognize a predefined data type, and if it is to be encrypted, to encrypt the payload portion of the packet data; and
a data combiner configured to combine the encrypted payload portion of the packet data with the non-payload portion of the packet data, wherein the non-payload portion of the packet data includes more than routing information.
2. (Currently Amended) The apparatus of claim 1, wherein the packet data includes streaming data.
3. (Canceled)
4. (Currently Amended) The apparatus of claim 1, wherein the non-payload portion of the packet data includes at least one of a header, control data and routing data.
5. (Currently Amended) The apparatus of claim 1, further comprising a transmitter configured to send the combined payload and non-payload portions of the packet data over the network to the client.
6. (Currently Amended) The apparatus of claim 1, further comprising a receiver configured to receive the data from the server before the data is sent in the packet over the network to the client.
7. (Previously Presented) The apparatus of claim 1, further comprising a device configured to establish a data stream between the server and the client.

{S:\08223\000S102-US0\80064057.DOC / }

8. (Previously Presented) The apparatus of claim 1, further comprising a key negotiator configured to negotiate an encryption key with the client.

9. (Previously Presented) The apparatus of claim 8, wherein key negotiation and key exchange occur during transmission of a stream.

10. (Previously Presented) The apparatus of claim 9, wherein the encrypter is transparent to the server.

11. (Previously Presented) The apparatus of claim 8, wherein key negotiation can determine if the encryption key is current.

12. (Currently Amended) The apparatus of claim 1, further comprising a decrypter configured to decrypt the encrypted payload portion of the packet data at the client.

13. (Currently Amended) The apparatus of claim 1, wherein the parser is further configured to parse the packet data into different portions based on a media format.

14. (Currently Amended) The apparatus of claim 1, wherein the encrypter is further configured to encrypt the payload portion of the packet data based on a media format.

15. (Currently Amended) The apparatus of claim 1, wherein the apparatus is implemented utilizing an application that includes a pluggable core encoding an encryption algorithm for encrypting the payload portion of the packet data, wherein the pluggable core enables the encryption algorithm to be readily changed.

16. (Previously Presented) The apparatus of claim 1, wherein the apparatus is implemented on an encryption bridge.

17. (Currently Amended) A method for selectively encrypting data in a packet received from a data source, the data including payload and non-payload portions which differ from each

{S:\08223\000S102-US0\80064057.DOC \[REDACTED] }

other in at least one characteristic, the received data to be subsequently sent over a network to a client, the method comprising:

parsing the received packet data into portions including the payload and non-payload portions;

determining if the payload portion is to be encrypted based on a format of the payload portion of the packet data by examining the payload portion of the packet data to recognize a predefined data type, and if it is to be encrypted, encrypting the payload portion of the received packet data; and

sending the received packet data including the encrypted payload portion and the non-payload portion of the received packet data over the network to the client.

18. (Previously Presented) The method of claim 17, wherein the data source is a server.

19. (Previously Presented) The method of claim 17, further comprising determining whether a stream is established between a server and the client.

20. (Previously Presented) The method of claim 17, further comprising negotiating an encryption key with the client.

21. (Currently Amended) The method of claim 20, wherein the received packet data from the data source is streaming data sent during a streaming session and the negotiating of the encryption key is carried out during the streaming session.

22. (Currently Amended) The method of claim 20, wherein the received packet data from the data source is streaming data sent during a streaming session, the method further comprising examining the client during the streaming session and terminating the streaming session if the encryption key on the client is invalid.

23. (Previously Presented) The method of claim 20, wherein the encryption key is negotiated with a decryption shim on the client.

{S:\08223\000S102-US0\80064057.DOC 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 160 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191 192 193 194 195 196 197 198 199 200 201 202 203 204 205 206 207 208 209 210 211 212 213 214 215 216 217 218 219 220 221 222 223 224 225 226 227 228 229 230 231 232 233 234 235 236 237 238 239 240 241 242 243 244 245 246 247 248 249 250 251 252 253 254 255 256 257 258 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274 275 276 277 278 279 280 281 282 283 284 285 286 287 288 289 290 291 292 293 294 295 296 297 298 299 300 301 302 303 304 305 306 307 308 309 310 311 312 313 314 315 316 317 318 319 320 321 322 323 324 325 326 327 328 329 330 331 332 333 334 335 336 337 338 339 340 341 342 343 344 345 346 347 348 349 350 351 352 353 354 355 356 357 358 359 360 361 362 363 364 365 366 367 368 369 370 371 372 373 374 375 376 377 378 379 380 381 382 383 384 385 386 387 388 389 390 391 392 393 394 395 396 397 398 399 400 401 402 403 404 405 406 407 408 409 410 411 412 413 414 415 416 417 418 419 420 421 422 423 424 425 426 427 428 429 430 431 432 433 434 435 436 437 438 439 440 441 442 443 444 445 446 447 448 449 450 451 452 453 454 455 456 457 458 459 460 461 462 463 464 465 466 467 468 469 470 471 472 473 474 475 476 477 478 479 480 481 482 483 484 485 486 487 488 489 490 491 492 493 494 495 496 497 498 499 500 501 502 503 504 505 506 507 508 509 510 511 512 513 514 515 516 517 518 519 520 521 522 523 524 525 526 527 528 529 530 531 532 533 534 535 536 537 538 539 540 541 542 543 544 545 546 547 548 549 550 551 552 553 554 555 556 557 558 559 560 561 562 563 564 565 566 567 568 569 570 571 572 573 574 575 576 577 578 579 580 581 582 583 584 585 586 587 588 589 590 591 592 593 594 595 596 597 598 599 600 601 602 603 604 605 606 607 608 609 610 611 612 613 614 615 616 617 618 619 620 621 622 623 624 625 626 627 628 629 630 631 632 633 634 635 636 637 638 639 640 641 642 643 644 645 646 647 648 649 650 651 652 653 654 655 656 657 658 659 660 661 662 663 664 665 666 667 668 669 670 671 672 673 674 675 676 677 678 679 680 681 682 683 684 685 686 687 688 689 690 691 692 693 694 695 696 697 698 699 700 701 702 703 704 705 706 707 708 709 710 711 712 713 714 715 716 717 718 719 720 721 722 723 724 725 726 727 728 729 730 731 732 733 734 735 736 737 738 739 740 741 742 743 744 745 746 747 748 749 750 751 752 753 754 755 756 757 758 759 760 761 762 763 764 765 766 767 768 769 770 771 772 773 774 775 776 777 778 779 780 781 782 783 784 785 786 787 788 789 790 791 792 793 794 795 796 797 798 799 800 801 802 803 804 805 806 807 808 809 810 811 812 813 814 815 816 817 818 819 820 821 822 823 824 825 826 827 828 829 830 831 832 833 834 835 836 837 838 839 840 841 842 843 844 845 846 847 848 849 850 851 852 853 854 855 856 857 858 859 860 861 862 863 864 865 866 867 868 869 870 871 872 873 874 875 876 877 878 879 880 881 882 883 884 885 886 887 888 889 890 891 892 893 894 895 896 897 898 899 900 901 902 903 904 905 906 907 908 909 910 911 912 913 914 915 916 917 918 919 920 921 922 923 924 925 926 927 928 929 930 931 932 933 934 935 936 937 938 939 940 941 942 943 944 945 946 947 948 949 950 951 952 953 954 955 956 957 958 959 960 961 962 963 964 965 966 967 968 969 970 971 972 973 974 975 976 977 978 979 980 981 982 983 984 985 986 987 988 989 990 991 992 993 994 995 996 997 998 999 1000 1001 1002 1003 1004 1005 1006 1007 1008 1009 1010 1011 1012 1013 1014 1015 1016 1017 1018 1019 1020 1021 1022 1023 1024 1025 1026 1027 1028 1029 1030 1031 1032 1033 1034 10

24. (Currently Amended) The method of claim 17, further comprising determining whether the received packet data is streaming data.

25. (Currently Amended) The method of claim 24, further comprising parsing, encrypting and sending the packet data if the packet data is streaming data and sending the packet data if the packet data is not streaming data.

26. (Previously Presented) The method of claim 17, further comprising determining whether a shim is present on the client.

27. (Previously Presented) The method of claim 26, further comprising sending a shim to the client if it is determined that the shim is not present on the client.

28. (Previously Presented) The method of claim 17, further comprising determining whether an encryption key on the client is current.

29. (Currently Amended) The method of claim 17, wherein the packet data includes at least one of a header, control data and routing data.

30. (Canceled)

31. (Currently Amended) The method of claim 17, wherein the packet data received from the data source for sending to the client is a stream of packets, the method further comprising determining whether a particular packet is the last packet in a data stream.

32. (Currently Amended) The method of claim 31, further comprising receiving feedback from a decryption shim on the client if it is determined that the particular packet is not the last packet in the data stream.

33. (Previously Presented) The method of claim 17, further comprising determining whether the client is compromised.

{S:\08223\000S102-US0\80064057.DOC 11:40:00 AM 05/23/2006 }

34. (Currently Amended) The method of claim 33, further comprising continuing parsing, encrypting and sending the packet data into the payload and non-payload portions if it is determined that the client is not compromised.

35. (Previously Presented) The method of claim 33, further comprising terminating the sending to the client if it is determined that the client is compromised.

36. (Currently Amended) A method for streaming data at a client, the data including payload and non-payload portions which differ from each other in at least one characteristic, the streaming data is included in a plurality of packets having been sent over a network to the client from an encryption source, the method comprising:

receiving the packet data sent over the network;
parsing the packet data into portions including the payload and non-payload portions;
if the payload portion of the packet data is encrypted based on a format of the payload portion of the packet data, as determined by an examination of the payload portion of the packet data to recognize a predefined data type, decrypting the payload portion of the packet data; and
passing the decrypted payload portion of the packet data to a higher level of operations for play in the client.

37. (Currently Amended) The method of claim 36, further comprising prior to the parsing, determining whether the packet data is an unencrypted stream.

38. (Currently Amended) The method of claim 37, further comprising passing the packet data to a higher level of operations without parsing and decrypting ~~when~~ if it is determined that the packet data is an unencrypted stream.

39. (Previously Presented) The method of claim 36, further comprising negotiating a decryption key with the encryption source.

40. (Previously Presented) The method of claim 39, wherein the streaming data is sent from the encryption source during a streaming session and said negotiating the decryption key is carried out during the streaming session.

41. (Previously Presented) The method of claim 39, further comprising terminating a stream if the decryption key is invalid.

42. (Canceled)

43. (Currently Amended) The method of claim 36, wherein the packet data is sent from the encryption source over the network as a stream of data packets, the method further comprising determining whether a particular packet received by the client is a last packet in a data stream.

44. (Currently Amended) The method of claim 43, further comprising sending feedback to the encryption source if it is determined that the particular packet is not the last packet in the data stream.

45. (Previously Presented) The method of claim 36, further comprising determining whether the client is compromised.

46. (Currently Amended) The method of claim 45, further comprising continuing the parsing, decrypting and passing the packet data as aforesaid if it is determined that the client is not compromised.

47. (Previously Presented) The method of claim 45, further comprising terminating a streaming session if it is determined that the client is compromised.

48. (Currently Amended) The apparatus of claim 1, wherein the payload packet data includes multimedia data.

49. (Currently Amended) The apparatus of claim 1, wherein the parser is further configured to parse the packet data into different portions based on a data protocol used to transmit a data stream of packets.

50. (Currently Amended) The apparatus of claim ~~[[1]]~~ 36, wherein the parser parses the packet data based on ~~[[the]]~~ a data protocol.

51. (Currently Amended) The method of claim 41, wherein the terminating of the encrypted stream includes sending a feedback signal to the encryption source instructing to stop sending the packet data over the network.

52. (Previously Presented) The method of claim 36, further comprising terminating a streaming session based on a determination that the client is compromised.

53. (Currently Amended) A method for selectively encrypting data for transmission over a network, the method comprising:

examining the data of each received packet to identify a plurality of portions that include at least a payload portion and a non-payload portion;

determining if at least one of the payload portion is to be encrypted by examining the at least one payload portion to recognize a predefined data type, and if the at least one payload portion is to be encrypted, encrypting the at least one payload portion; and

at least another portion of the packet to remain unencrypted, wherein the plurality of portions of encrypted payload and non-payload for a packet being combined after such encryption determination.

54. (Currently Amended) The method of claim 53, wherein the packet data is received from a data source, wherein the packet data includes streaming data and wherein the at least one data portion of a packet to remain unencrypted includes at least one of a header, control data and routing data.

55. (Currently Amended) The method of claim 54, wherein the streaming data is included in the at least one data portion of the packet to remain unencrypted.

56. (Currently Amended) The method of claim 55, further comprising:
transmitting the combined packet data over the network to a client; and
negotiating and exchanging a key with the client before the combined data is transmitted over the network to the client, the key enabling the client to decrypt the encrypted portion of the packet data for play on the client.


57. (Previously Presented) The method of claim 56, wherein the streaming data is sent during a streaming session and wherein the negotiating and exchanging the key is carried out during the streaming session.

58. (Previously Presented) The method of claim 57, further comprising examining the client during the streaming session and terminating the streaming session if the key on the client is invalid.

59. (Currently Amended) The method of claim 58, wherein the data source is a server and the examining of the packet data is carried out on an encryption bridge between the server and the network so that the examining of the packet data, encrypting and combining of the plurality of data portions is transparent to the server.

60. (Previously Presented) The method of claim 59, wherein the key negotiating and exchanging and the decryption using the key is carried out using a shim on the client, the shim being configured so that the negotiating and exchanging of the key thereby and the decrypting of the data thereby is transparent to the client.

61. (Currently Amended) An apparatus for selectively encrypting streaming data packets received from a streaming data source for transmission over a network to a client, the apparatus comprising:

{S:\08223\000S102-US0\80064057.DOC  }

a parser configured to parse a plurality of portions of the streaming data packets,
wherein the plurality of portions include a payload portion and a non-payload portion in each of
the streaming data packets;

an encrypter configured to encrypt at least ~~[[a]]~~ the payload portion if it is
determined, based on an examination of a format of the ~~[[the]]~~ payload portion to recognize a
predefined data type, payload portion is to be encrypted, but not encrypt at least one other data
portion of the plurality of data portions; and

a data combiner configured to combine the encrypted payload portion with at least
one unencrypted non-payload data portion.

62. (Currently Amended) The apparatus of claim 61, further comprising a negotiator,
wherein the negotiator negotiates and exchanges a key with the client before the combined
packet data is transmitted over the network to the client, the key enabling the client to decrypt the
encrypted payload portion of the packet data for play on the client.


63. (Previously Presented) The apparatus of claim 62, wherein the streaming data is
sent from the streaming data source during a streaming session.

64. (Previously Presented) The apparatus of claim 63, further configured to perform
actions including examining the client during the streaming session and terminating the
streaming session if the client has been compromised.

65. (Currently Amended) The apparatus of claim 61, wherein the at least one
unencrypted data portion of the packet data includes at least one of a header, control data and
routing data.

66. (Previously Presented) The apparatus of claim 61, wherein the streaming data
source is at least one server.

67. (Currently Amended) An apparatus for selectively encrypting data received from
a data source for transmission in packets over a network to a client, comprising:

{S:\08223\000S102-US0\80064057.DOC / }

a parser configured to parse at least two portions of the packet data, at least one of the two portions of the packet data including more than routing information for a packet;

an encrypter configured to determine if ~~only one~~ a payload portion of the packet data is to be encrypted based on an examination of ~~only the one~~ payload portion the packet data to recognize a predefined data type, and if it is to be encrypted, encrypting ~~only the~~ payload ~~one~~ portion of packet data not including the routing information for the packet; and

a data combiner configured to combine the parsed at least two portions of the packet data following encryption of the ~~one~~ payload portion of data not including the routing information for the packet.

68. (Currently Amended) The apparatus of claim 67, wherein ~~[[the]]~~an unencrypted portion of the packet data includes at least one of a header and control data.

69. (Previously Presented) The apparatus of claim 68, wherein the parser parses the data into different portions based on a data protocol used to transmit the data.

70. (Currently Amended) The apparatus of claim 68, wherein the portion of the packet data to be encrypted includes media data encoded in a media format and wherein the encrypter encrypts the packet data to be encrypted based on the media format.

71. (Currently Amended) The apparatus of claim 70, wherein the apparatus is implemented utilizing an application that includes a pluggable core encoding an encryption algorithm for encrypting the packet data, the pluggable core being replaceable to enable the encryption algorithm to be readily changed.

72. (Previously Presented) The apparatus of claim 71, wherein the apparatus is implemented on an encryption bridge.

73. (Currently Amended) An apparatus for selectively encrypting data received from a data source during a downloading operation, the data being received from the data source for

transmission in packets over a network to a client receiving the downloaded packetized data, comprising:

a parser configured to parse at least two portions of the data in a packet, wherein the packet data includes a payload portion and a non-payload portion;

an encrypter configured to determine if ~~[[a]]~~ the payload portion of the packet data is to be encrypted based on a format of the payload portion of the packet data, wherein the format is determined based on an examination of the payload portion of the packet data to recognize a predefined data type, and if it is to be encrypted, encrypting ~~only~~ the payload portion of the packet data; and

a data combiner configured to combine the encrypted payload portion of the packet data with an unencrypted portion of packet data for transmission over the network.


74. (Currently Amended) The apparatus as defined in claim 73, wherein the downloaded data is included in the encrypted payload portion of the packet data.

75. (Currently Amended) The apparatus of claim 74, wherein the unencrypted portion of packet data includes at least one of a header, control data and routing data.

76. (Currently Amended) The apparatus of claim 75, further comprising a key negotiator configured to perform actions including negotiating and exchanging a key with the client before the packet data is sent over the network to the client, the key enabling the client to decrypt the encrypted payload portion of data.

77. (Canceled)

78. (Currently Amended) An apparatus for selectively encrypting data, received from a data source during a downloading operation and for selectively encrypting data received in packets from a data source during a streaming operation, the packet data being received from the data source for transmission over a network to a client receiving the downloaded or streaming data, comprising:

{S:\08223\000S102-US0\80064057.DOC  }

a means for parsing at least two portions of the data included in a packet, wherein the packet data comprises at least a payload portion and a non-payload portion;

a means for determining if ~~[[a]]~~the payload portion of the at least two portions of data is to be encrypted based on a format of the one portion of packet data that is determined by recognizing a predefined data type in the payload portion of the at least two portions, and if the a payload portion of data is to be encrypted, employing a means for encrypting only the payload portion of the at least two portions of data; and

a means for combining the encrypted payload portion of the packet data with ~~[[the]]~~ at least the unencrypted portion of the packet data for transmission over the network.

79. (Currently Amended) The apparatus of claim 78, wherein during the streaming operation, the streaming data is included in the packet data portion that is to be encrypted.

80. (Currently Amended) The apparatus as defined in claim 79, further comprising a key negotiating means configured to negotiate and exchange a key with the client before the streaming data is sent over the network to the client, the key enabling the client to decrypt the encrypted payload portion of the packet data for play on the client.

81. (Canceled)

82. (Previously Presented) The apparatus of claim 78, further comprising a client examining means configured to examine the client during a streaming session and terminate the streaming session if the client has been compromised.

83. (Currently Amended) The apparatus of claim 82, wherein the packet data portion that is not encrypted includes at least one of a header, control data and routing data.

84. (Currently Amended) The apparatus of claim 78, wherein during a downloading operation, the downloaded data is included in the packet data portion that is to be encrypted.

85. (Previously Presented) The apparatus of claim 84, wherein the data portion that is not encrypted includes at least one of a header, control data and routing data.

86. (Currently Amended) A shim deployed on a client, the shim comprising:
a data receiver configured to receive partially encrypted packet data transmitted to the client, wherein another device parsed the packet data into a payload portion and a non-payload portion and determined [[a]]the payload portion of the packet data to be encrypted based on a format of the payload portion of the packet data, wherein the format is determined by an examination of that payload portion of the packet data to recognize a predefined data type~~[[.]]~~;
a parser configured to parse the partially encrypted packet data to select the payload portion of the packet data to be decrypted;
a decrypter configured to decrypt the payload portion of the packet data selected for decrypting by the parser; and
a data transmitter configured to send the decrypted packet data to a higher level operation resident on the client.

87. (Currently Amended) The shim of claim 86, wherein an encrypted portion of the transmitted packet data includes media data, the data transmitter being further configured to send the decrypted media data to a media player resident on the client.

88. (Previously Presented) The shim of claim 87, wherein the media data is streaming media transmitted to the client during a streaming session.

89. (Currently Amended) The shim of claim 88, wherein the unencrypted portion of the packet data includes at least one of a header, control data and routing data.

90. (Previously Presented) The shim of claim 88, further comprising an analyzer configured to analyze a behavior of the client to detect known media piracy techniques and to terminate the streaming session if a known media piracy technique is detected.

91. (Previously Presented) The shim of claim 88, further comprising an analyzer configured to analyze a behavior of the client to detect suspicious client behavior and to terminate the streaming session if specific behavior is detected.

92. (Previously Presented) The shim of claim 88, further comprising an analyzer configured to analyze a behavior of the client to detect known media piracy techniques and to terminate operation of at least the decrypter when a media piracy technique is detected.

93. (Previously Presented) The shim of claim 88, further comprising an analyzer configured to analyze a behavior of the client to detect suspicious client behavior and to terminate the operation of at least the decrypter if suspicious behavior is detected.


94. (Currently Amended) The shim of claim 88, further comprising a key negotiator configured to negotiate and exchange a key with the client before the packet data is sent over the network to the client, the key enabling the client to decrypt the encrypted portion of the packet data for play on the client.

95. (Currently Amended) The shim of claim 88, wherein the streaming data is sent to the client from an encryption source, the shim further including a key negotiator configured to negotiate and exchange a key with the encryption source, the key being used by the decrypter to decrypt the encrypted portion of the packet data.

96. (Previously Presented) The shim of claim 95 wherein the key negotiator is further configured to carry out the negotiating and exchanging of the key with the encryption source during the streaming session.

97. (Currently Amended) A method for providing data in packets over a network, comprising:

determining a plurality of portions of [[the]]data in a packet that includes a payload portion and a non-payload portion;

{S:\08223\000S102-US0\80064057.DOC / }

